ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

Кафедра
«Криптология и кибербезопасность»

Лабораторная работа №8

по предмету «Технологии контейнеризации»

Выполнил студент группы Б20-505

Сорочан Илья

Москва – 2023

Содержание

1. Выбор образа

Выбрал kassany/ziglang

Тэг master

```
vagrant@delta:~$ sudo docker pull kassany/ziglang
Using default tag: latest
latest: Pulling from kassany/ziglang
ff6c6006db95: Pull complete
ed62fc66e749: Pull complete
Digest: sha256:232a2fdcc53efbd78218928e63bc9748f03b588459b2ee3186cd04a2e119fcbc
Status: Downloaded newer image for kassany/ziglang:latest
docker.io/kassany/ziglang:latest
```

Рис. 1. Скачивание образа

```
vagrant@delta:~$ sudo docker run --rm -v $(pwd):/app -w /app kassany/ziglang
info: Usage: zig [command] [options]

Commands:

  build            Build project from build.zig
  fetch            Copy a package into global cache and print its hash
  init-exe         Initialize a `zig build` application in the cwd
  init-lib         Initialize a `zig build` library in the cwd

  ast-check        Look for simple compile errors in any set of files
  build-exe        Create executable from source or object files
  build-lib        Create library from source or object files
  build-obj        Create object from source or object files
  fmt              Reformat Zig source into canonical form
  run              Create executable and run immediately
  test             Create and run a test build
  translate-c      Convert C code to Zig code

  ar               Use Zig as a drop-in archiver
  cc               Use Zig as a drop-in C compiler
  c++              Use Zig as a drop-in C++ compiler
  dlltool          Use Zig as a drop-in dlltool.exe
  lib              Use Zig as a drop-in lib.exe
  ranlib           Use Zig as a drop-in ranlib
  objcopy          Use Zig as a drop-in objcopy
  rc               Use Zig as a drop-in rc.exe

  env              Print lib path, std path, cache directory, and version
  help             Print this help and exit
  libc             Display native libc paths file or validate one
  targets          List available compilation targets
  version          Print version number and exit
  zen              Print Zen of Zig and exit

General Options:

  -h, --help       Print command-specific usage

error: expected command argument
```

Рис. 2. Запуск образа

2. Сканирование

2.1. Docker Scout

```
curl -fsSL https://raw.githubusercontent.com/docker/scout-cli/main/install.sh | sh
```

```
vagrant@delta:~$ docker scout
docker: 'scout' is not a docker command.
See 'docker --help'
vagrant@delta:~$ curl -fsSL https://raw.githubusercontent.com/docker/scout-cli/main/install.sh | sh
[info] fetching release script for tag='v1.0.9'
[info] using release tag='v1.0.9' version='1.0.9' os='linux' arch='amd64'
[info] installed /home/vagrant/.docker/cli-plugins/docker-scout
vagrant@delta:~$ docker scout --help

 Command line tool for Docker Scout

Usage
  docker scout [command]

Available Commands
  cache           Manage Docker Scout cache and temporary files
  compare         Compare two images and display differences (experimental)
  config          Manage Docker Scout configuration
  cves            Display CVEs identified in a software artifact
  enroll          Enroll an organization with Docker Scout
  environment     Manage environments (experimental)
  help            Display information about the available commands
  integration     Commands to list, configure, and delete Docker Scout integrations
  policy          Evaluate policies against an image and display the policy evaluation results (experimental)
  quickview       Quick overview of an image
  recommendations Display available base image updates and remediation recommendations
  repo            Commands to list, enable, and disable Docker Scout on repositories
  version         Show Docker Scout version information

Use "docker scout [command] --help" for more information about a command.

Learn More
  Read docker scout cli reference at https://docs.docker.com/engine/reference/commandline/scout/

Report Issues
  Raise bugs and feature requests at https://github.com/docker/scout-cli/issues
```

Рис. 3. Установка Docker Scout

```
vagrant@delta:~$ docker scout quickview kassane/ziglang
Log in with your Docker ID or email address to use docker scout.

If you don't have a Docker ID, head over to https://hub.docker.com to
create one. You can log in with your password or a Personal Access Token (PAT)
by running docker login.
Using a limited-scope PAT grants better security and is required for organizations
using SSO. Learn more at https://docs.docker.com/go/access-tokens/

You can also log in using Docker Desktop.
```

Рис. 4. Docker Scout Quickview

```
vagrant@delta:~$ docker image ls
REPOSITORY        TAG       IMAGE ID       CREATED      SIZE
kassany/ziglang   latest    784730331869   2 days ago   285MB
vagrant@delta:~$ docker tag kassany/ziglang:latest k0tran/ziglang:latest
vagrant@delta:~$ docker image ls
REPOSITORY        TAG       IMAGE ID       CREATED      SIZE
k0tran/ziglang    latest    784730331869   2 days ago   285MB
kassany/ziglang   latest    784730331869   2 days ago   285MB
```

Рис. 5. Ретегаем

```
vagrant@delta:/vagrant$ docker login -u k0tran
Password:
WARNING! Your password will be stored unencrypted in /home/vagrant/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
```

Рис. 6. Логинимся

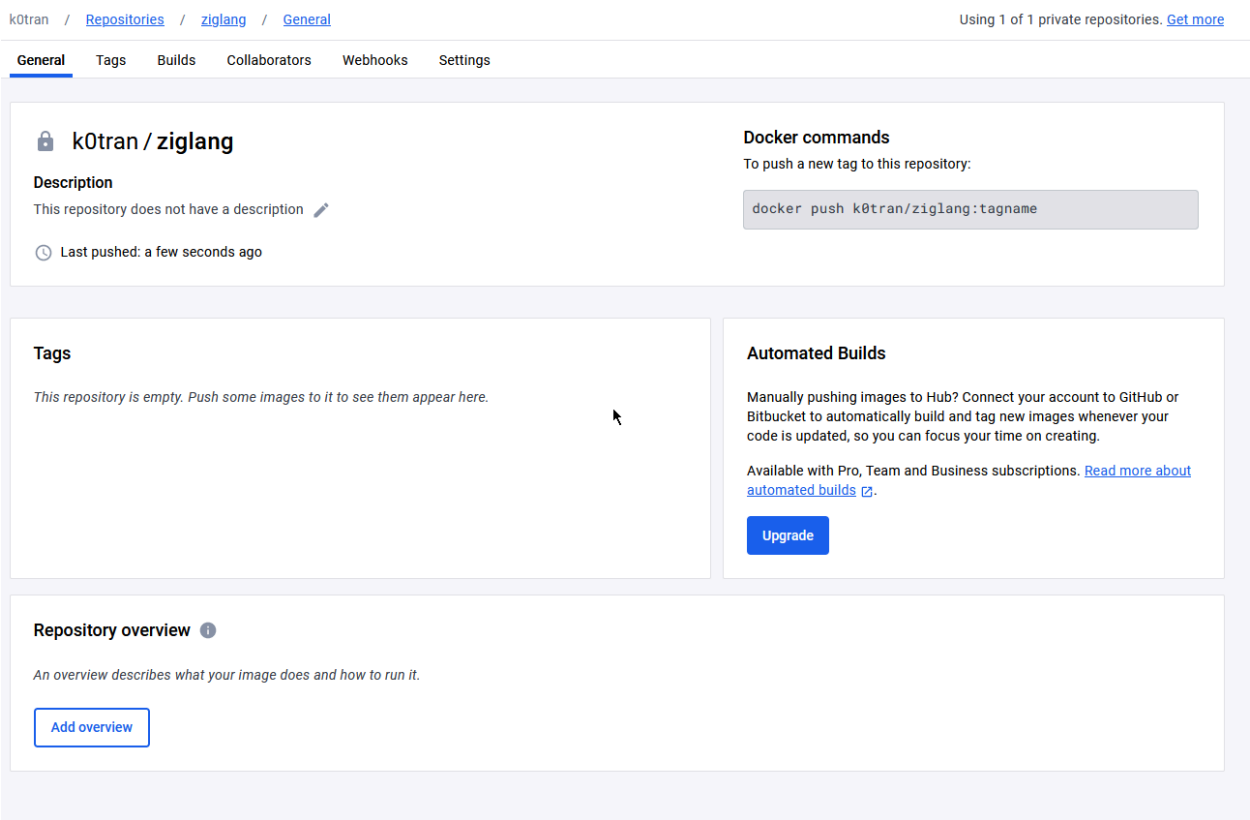


Рис. 7. Создаем репозиторий

```
vagrant@delta:~$ docker push k0tran/ziglang
Using default tag: latest
The push refers to repository [docker.io/k0tran/ziglang]
77fd90906824: Pushed
bd16786bcaea: Pushed
latest: digest: sha256:f0974b8c86bc78d9db238812fab0e3c0cc7c0b41930c97a158c550119536cd67 size: 740
```

Рис. 8. Пушим

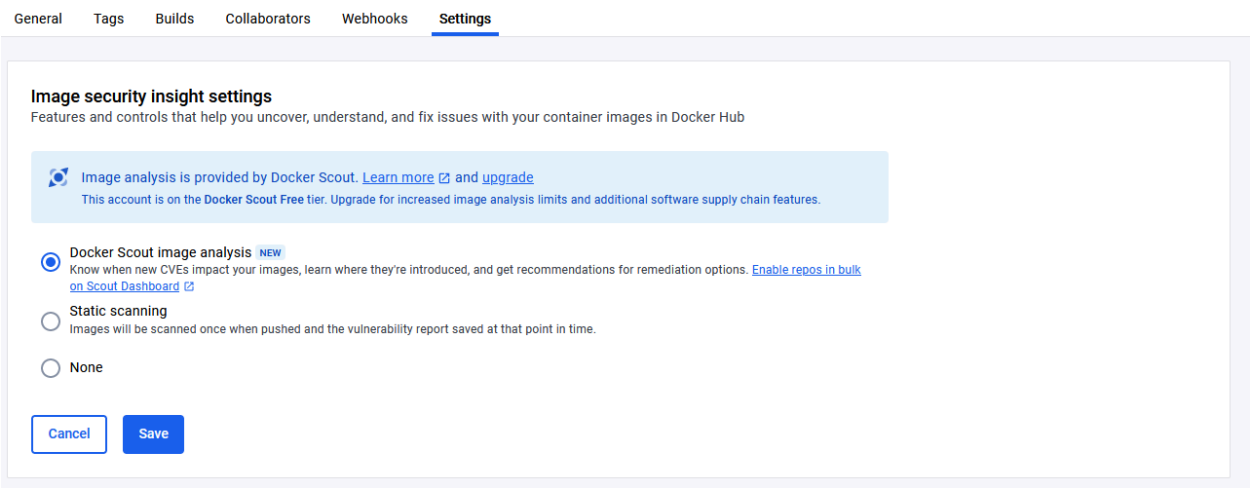


Рис. 9. Врубаем Docker Scout

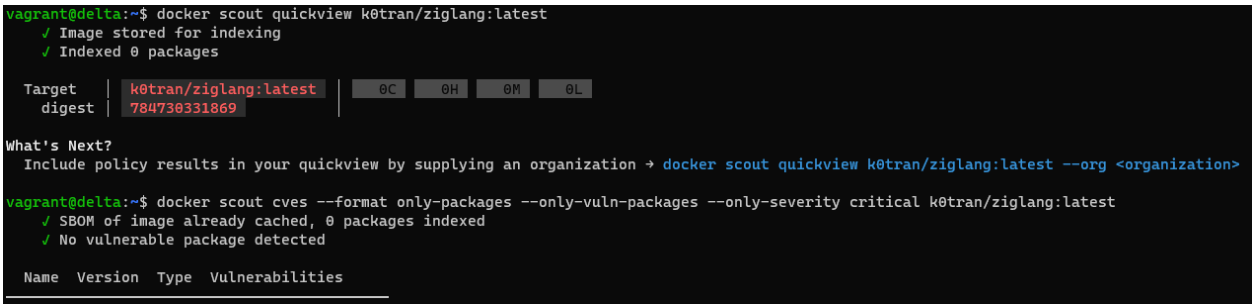


Рис. 10. Смотрим уязвимости

2.2. Snyk

```
sudo apt install npm -y
sudo npm install snyk -g -y
```

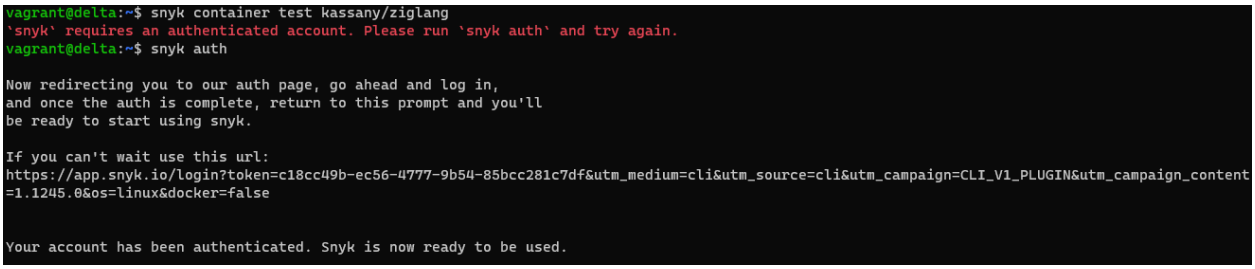


Рис. 11. Логинимся в snyk

```
vagrant@delta:~$ snyk container test kassany/ziglang

Testing kassany/ziglang...

Organization:      k0tran
Package manager:   linux
Project name:      docker-image|kassany/ziglang
Docker image:      kassany/ziglang
Platform:          linux/amd64
Licenses:          enabled

✓ Tested kassany/ziglang for known issues, no vulnerable paths found.

Note that we do not currently have vulnerability data for your image.
```

Рис. 12. Анализ контейнера

2.3. Trivy

```
vagrant@delta:~$ sudo docker run aquasec/trivy
Unable to find image 'aquasec/trivy:latest' locally
latest: Pulling from aquasec/trivy
96526aa774ef: Pull complete
59cb99bf6343: Pull complete
326983ce57b1: Pull complete
a6abc1276873: Pull complete
Digest: sha256:275243b81dcc2728dd9b54125f62fa636528364f8d44b88b7d72ef47ac6ad86d
Status: Downloaded newer image for aquasec/trivy:latest
Scanner for vulnerabilities in container images, file systems, and Git repositories, as well as for configuration issues and hard-coded secrets

Usage:
  trivy [global flags] command [flags] target
  trivy [command]
```

Рис. 13. Используем контейнер

```
vagrant@delta:~$ sudo docker run --rm aquasec/trivy image kassany/ziglang
2023-11-14T11:08:56.135Z        INFO    Need to update DB
2023-11-14T11:08:56.135Z        INFO    DB Repository: ghcr.io/aquasecurity/trivy-db
2023-11-14T11:08:56.135Z        INFO    Downloading DB...
```

Рис. 14. Анализ контейнера (1)

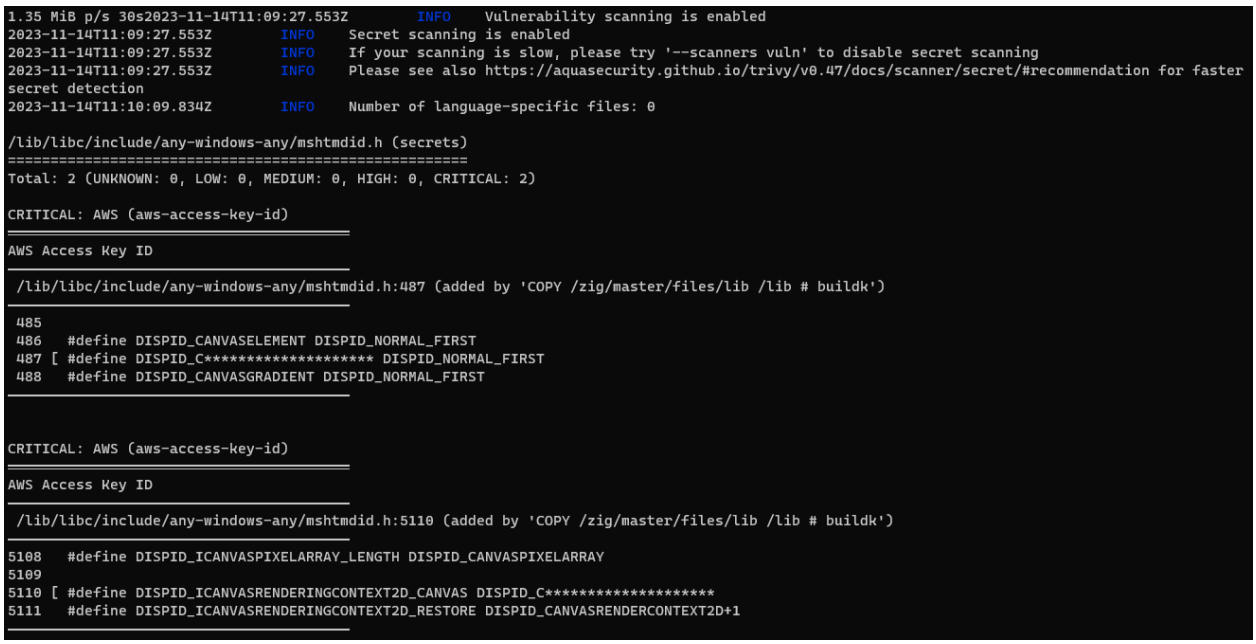


Рис. 15. Анализ контейнера (2)

Итого сканер нашел две уязвимости aws

2.4. anchore-engine

Репозиторий **заархивирован** в 2023

```
curl https://engine.anchore.io/docs/quickstart/docker-compose.yaml > docker-compose.yaml
docker-compose up -d
sudo apt-get install python3-pip -y
pip install anchorecli
export PATH=$PATH:/home/vagrant/.local/bin
```

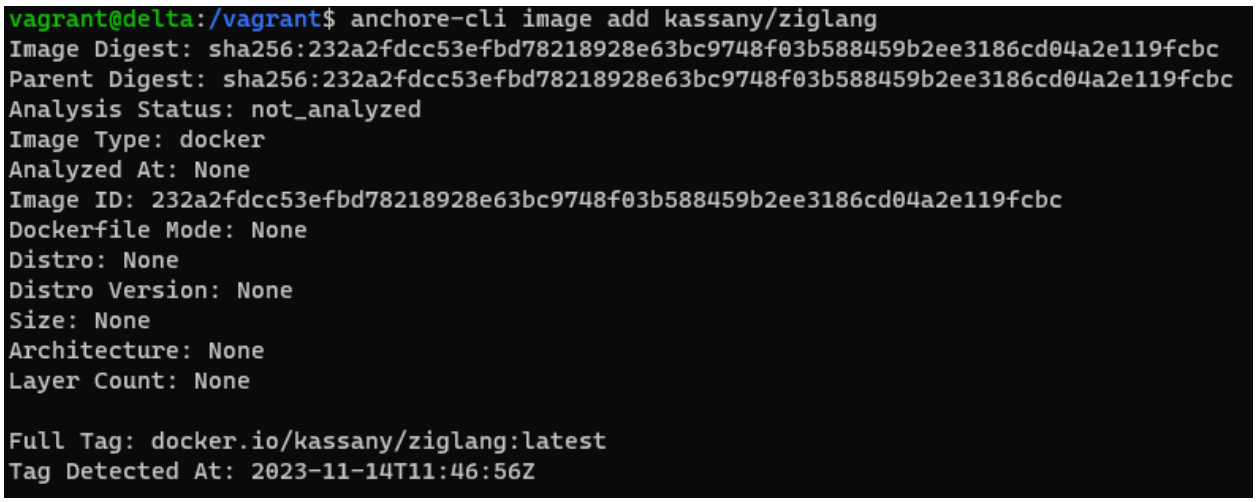


Рис. 16. Добавляем в очередь на анализ

```
vagrant@delta:/vagrant$ anchore-cli image wait kassany/ziglang
Image Digest: sha256:232a2fdcc53efbd78218928e63bc9748f03b588459b2ee3186cd04a2e119fcbc
Parent Digest: sha256:232a2fdcc53efbd78218928e63bc9748f03b588459b2ee3186cd04a2e119fcbc
Analysis Status: analysis_failed
Image Type: docker
Analyzed At: None
Image ID: 232a2fdcc53efbd78218928e63bc9748f03b588459b2ee3186cd04a2e119fcbc
Dockerfile Mode: None
Distro: None
Distro Version: None
Size: None
Architecture: None
Layer Count: None

Full Tag: docker.io/kassany/ziglang:latest
Tag Detected At: 2023-11-14T11:46:56Z


vagrant@delta:/vagrant$ anchore-cli image list
Full Tag                              Image Digest                                                              Analysis Status
docker.io/kassany/ziglang:latest      sha256:232a2fdcc53efbd78218928e63bc9748f03b588459b2ee3186cd04a2e119fcbc   analysis_failed
```

Рис. 17. Анализ зафейлен

```
vagrant@delta:/vagrant$ anchore-cli image list
Full Tag                              Image Digest                                                              Analysis Status
docker.io/kassany/ziglang:latest      sha256:232a2fdcc53efbd78218928e63bc9748f03b588459b2ee3186cd04a2e119fcbc   not_analyzed
vagrant@delta:/vagrant$ anchore-cli image list
Full Tag                              Image Digest                                                              Analysis Status
docker.io/kassany/ziglang:latest      sha256:232a2fdcc53efbd78218928e63bc9748f03b588459b2ee3186cd04a2e119fcbc   analyzing
vagrant@delta:/vagrant$ anchore-cli image list
Full Tag                              Image Digest                                                              Analysis Status
docker.io/kassany/ziglang:latest      sha256:232a2fdcc53efbd78218928e63bc9748f03b588459b2ee3186cd04a2e119fcbc   analyzing
vagrant@delta:/vagrant$ anchore-cli image wait kassany/ziglang
Image Digest: sha256:232a2fdcc53efbd78218928e63bc9748f03b588459b2ee3186cd04a2e119fcbc
Parent Digest: sha256:232a2fdcc53efbd78218928e63bc9748f03b588459b2ee3186cd04a2e119fcbc
Analysis Status: analysis_failed
Image Type: docker
Analyzed At: None
Image ID: 232a2fdcc53efbd78218928e63bc9748f03b588459b2ee3186cd04a2e119fcbc
Dockerfile Mode: None
Distro: None
Distro Version: None
Size: None
Architecture: None
Layer Count: None

Full Tag: docker.io/kassany/ziglang:latest
Tag Detected At: 2023-11-14T11:46:56Z
```

Рис. 18. Пытался перезапустить, но catalog чет отваливается

Попробуем загрузить какой-нибудь другой, более простой образ:

```
vagrant@delta:~$ anchore-cli --u admin --p foobar image add hello-world
Image Digest: sha256:ac69084025c660510933cca701f615283cdbb3aa0963188770b54c31c8962493
Parent Digest: sha256:ac69084025c660510933cca701f615283cdbb3aa0963188770b54c31c8962493
Analysis Status: not_analyzed
Image Type: docker
Analyzed At: None
Image ID: ac69084025c660510933cca701f615283cdbb3aa0963188770b54c31c8962493
Dockerfile Mode: None
Distro: None
Distro Version: None
Size: None
Architecture: None
Layer Count: None

Full Tag: docker.io/hello-world:latest
Tag Detected At: 2023-12-17T22:35:11Z
```

Рис. 19. Запуск анализа

```
vagrant@delta:~$ anchore-cli --u admin --p foobar image list
Error: failed get url=http://catalog:8228/v1/images
HTTP Code: 500
Detail: {'error_codes': []}

vagrant@delta:~$ sudo docker ps
CONTAINER ID   IMAGE                              COMMAND                  CREATED         STATUS                    PORTS                                       NAMES
fb8024fe4b64   anchore/anchore-engine:v1.0.0      "/docker-entrypoint.…"   3 minutes ago   Up 3 minutes (healthy)    8228/tcp                                    vagrant-queue-1
23b2da6e769f   anchore/anchore-engine:v1.0.0      "/docker-entrypoint.…"   3 minutes ago   Up 3 minutes (healthy)    8228/tcp                                    vagrant-policy-engine-1
acfac512d957   anchore/anchore-engine:v1.0.0      "/docker-entrypoint.…"   3 minutes ago   Up 3 minutes (healthy)    0.0.0.0:8228->8228/tcp, :::8228->8228/tcp   vagrant-api-1
df374c4022ab   anchore/anchore-engine:v1.0.0      "/docker-entrypoint.…"   3 minutes ago   Up 3 minutes (healthy)    8228/tcp                                    vagrant-analyzer-1
646f1f777864   anchore/anchore-engine:v1.0.0      "/docker-entrypoint.…"   3 minutes ago   Up 3 minutes (unhealthy)  8228/tcp                                    vagrant-catalog-1
2c560375bb41   postgres:9                         "docker-entrypoint.s…"   3 minutes ago   Up 3 minutes (healthy)    5432/tcp                                    vagrant-db-1
```

Рис. 20. Анализ зафейлен x2

После этого увеличим объем оперативки до 4096 и запустим анализ debian:

```
vagrant@delta:~$ anchore-cli --u admin --p foobar image get docker.io/library/debian:latest
Image Digest: sha256:0dc902c61cb495db4630a6dc2fa14cd45bd9f8515f27fbb12e3d73a119d30bf1
Parent Digest: sha256:bac353db4cc04bc672b14029964e686cd7bad56fe34b51f432c1a1304b9928da
Analysis Status: analyzed
Image Type: docker
Analyzed At: 2023-12-21T14:28:52Z
Image ID: 2a033a8c63712da54b5a516f5d69d41606cfb5c4ce9aa1690ee55fc4f9babb92
Dockerfile Mode: Guessed
Distro: debian
Distro Version: 12
Size: 128133120
Architecture: amd64
Layer Count: 1

Full Tag: docker.io/library/debian:latest
Tag Detected At: 2023-12-21T14:27:11Z
```

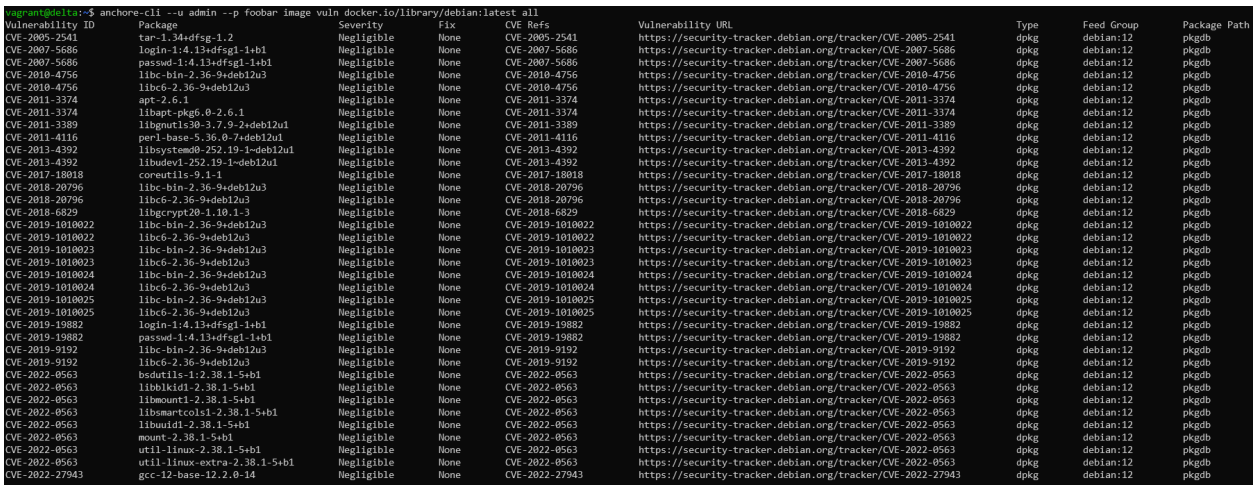
Рис. 21. Запуск анализа

```
vagrant@delta:~$ anchore-cli --u admin --p foobar image list
Full Tag                            Image Digest                                                                Analysis Status
docker.io/hello-world:latest        sha256:ac69084025c660510933cca701f615283cdbb3aa0963188770b54c31c8962493     analysis_failed
docker.io/library/debian:latest     sha256:0dc902c61cb495db4630a6dc2fa14cd45bd9f8515f27fbb12e3d73a119d30bf1     analyzed
```

Рис. 22. Анализ завершен

```
vagrant@delta:~$ anchore-cli --u admin --p foobar image vuln docker.io/library/debian:latest all | wc -l
48
```

Рис. 23. Число найденных уязвимостей



```
vagrant@delta:~$ anchore-cli --u admin --p foobar image vuln docker.io/library/debian:latest all
Vulnerability ID        Package                         Severity        Fix         CVE Refs            Vulnerability URL                                                   Type        Feed Group      Package Path
CVE-2005-2541           tar-1.34+dfsg-1.2               Negligible      None        CVE-2005-2541       https://security-tracker.debian.org/tracker/CVE-2005-2541           dpkg        debian:12       pkgdb
CVE-2007-5686           login-1:4.13+dfsg1-1+b1         Negligible      None        CVE-2007-5686       https://security-tracker.debian.org/tracker/CVE-2007-5686           dpkg        debian:12       pkgdb
CVE-2007-5686           passwd-1:4.13+dfsg1-1+b1        Negligible      None        CVE-2007-5686       https://security-tracker.debian.org/tracker/CVE-2007-5686           dpkg        debian:12       pkgdb
CVE-2010-4756           libc-bin-2.36-9+deb12u3         Negligible      None        CVE-2010-4756       https://security-tracker.debian.org/tracker/CVE-2010-4756           dpkg        debian:12       pkgdb
CVE-2010-4756           libc6-2.36-9+deb12u3            Negligible      None        CVE-2010-4756       https://security-tracker.debian.org/tracker/CVE-2010-4756           dpkg        debian:12       pkgdb
CVE-2011-3374           apt-2.6.1                       Negligible      None        CVE-2011-3374       https://security-tracker.debian.org/tracker/CVE-2011-3374           dpkg        debian:12       pkgdb
CVE-2011-3374           libapt-pkg6.0-2.6.1             Negligible      None        CVE-2011-3374       https://security-tracker.debian.org/tracker/CVE-2011-3374           dpkg        debian:12       pkgdb
CVE-2011-3389           libgnutls30-3.7.9-2+deb12u1     Negligible      None        CVE-2011-3389       https://security-tracker.debian.org/tracker/CVE-2011-3389           dpkg        debian:12       pkgdb
CVE-2011-4116           perl-base-5.36.0-7+deb12u1      Negligible      None        CVE-2011-4116       https://security-tracker.debian.org/tracker/CVE-2011-4116           dpkg        debian:12       pkgdb
CVE-2013-4392           libsystemd0-252.19-1~deb12u1    Negligible      None        CVE-2013-4392       https://security-tracker.debian.org/tracker/CVE-2013-4392           dpkg        debian:12       pkgdb
CVE-2013-4392           libudev1-252.19-1~deb12u1       Negligible      None        CVE-2013-4392       https://security-tracker.debian.org/tracker/CVE-2013-4392           dpkg        debian:12       pkgdb
CVE-2017-18018          coreutils-9.1-1                 Negligible      None        CVE-2017-18018      https://security-tracker.debian.org/tracker/CVE-2017-18018          dpkg        debian:12       pkgdb
CVE-2018-20796          libc-bin-2.36-9+deb12u3         Negligible      None        CVE-2018-20796      https://security-tracker.debian.org/tracker/CVE-2018-20796          dpkg        debian:12       pkgdb
CVE-2018-20796          libc6-2.36-9+deb12u3            Negligible      None        CVE-2018-20796      https://security-tracker.debian.org/tracker/CVE-2018-20796          dpkg        debian:12       pkgdb
CVE-2018-6829           libgcrypt20-1.10.1-3            Negligible      None        CVE-2018-6829       https://security-tracker.debian.org/tracker/CVE-2018-6829           dpkg        debian:12       pkgdb
CVE-2019-1010022        libc-bin-2.36-9+deb12u3         Negligible      None        CVE-2019-1010022    https://security-tracker.debian.org/tracker/CVE-2019-1010022        dpkg        debian:12       pkgdb
CVE-2019-1010022        libc6-2.36-9+deb12u3            Negligible      None        CVE-2019-1010022    https://security-tracker.debian.org/tracker/CVE-2019-1010022        dpkg        debian:12       pkgdb
CVE-2019-1010023        libc-bin-2.36-9+deb12u3         Negligible      None        CVE-2019-1010023    https://security-tracker.debian.org/tracker/CVE-2019-1010023        dpkg        debian:12       pkgdb
CVE-2019-1010023        libc6-2.36-9+deb12u3            Negligible      None        CVE-2019-1010023    https://security-tracker.debian.org/tracker/CVE-2019-1010023        dpkg        debian:12       pkgdb
CVE-2019-1010024        libc-bin-2.36-9+deb12u3         Negligible      None        CVE-2019-1010024    https://security-tracker.debian.org/tracker/CVE-2019-1010024        dpkg        debian:12       pkgdb
CVE-2019-1010024        libc6-2.36-9+deb12u3            Negligible      None        CVE-2019-1010024    https://security-tracker.debian.org/tracker/CVE-2019-1010024        dpkg        debian:12       pkgdb
CVE-2019-1010025        libc-bin-2.36-9+deb12u3         Negligible      None        CVE-2019-1010025    https://security-tracker.debian.org/tracker/CVE-2019-1010025        dpkg        debian:12       pkgdb
CVE-2019-1010025        libc6-2.36-9+deb12u3            Negligible      None        CVE-2019-1010025    https://security-tracker.debian.org/tracker/CVE-2019-1010025        dpkg        debian:12       pkgdb
CVE-2019-19882          login-1:4.13+dfsg1-1+b1         Negligible      None        CVE-2019-19882      https://security-tracker.debian.org/tracker/CVE-2019-19882          dpkg        debian:12       pkgdb
CVE-2019-19882          passwd-1:4.13+dfsg1-1+b1        Negligible      None        CVE-2019-19882      https://security-tracker.debian.org/tracker/CVE-2019-19882          dpkg        debian:12       pkgdb
CVE-2019-9192           libc-bin-2.36-9+deb12u3         Negligible      None        CVE-2019-9192       https://security-tracker.debian.org/tracker/CVE-2019-9192           dpkg        debian:12       pkgdb
CVE-2019-9192           libc6-2.36-9+deb12u3            Negligible      None        CVE-2019-9192       https://security-tracker.debian.org/tracker/CVE-2019-9192           dpkg        debian:12       pkgdb
CVE-2022-0563           bsdutils-1:2.38.1-5+b1          Negligible      None        CVE-2022-0563       https://security-tracker.debian.org/tracker/CVE-2022-0563           dpkg        debian:12       pkgdb
CVE-2022-0563           libblkid1-2.38.1-5+b1           Negligible      None        CVE-2022-0563       https://security-tracker.debian.org/tracker/CVE-2022-0563           dpkg        debian:12       pkgdb
CVE-2022-0563           libmount1-2.38.1-5+b1           Negligible      None        CVE-2022-0563       https://security-tracker.debian.org/tracker/CVE-2022-0563           dpkg        debian:12       pkgdb
CVE-2022-0563           libsmartcols1-2.38.1-5+b1       Negligible      None        CVE-2022-0563       https://security-tracker.debian.org/tracker/CVE-2022-0563           dpkg        debian:12       pkgdb
CVE-2022-0563           libuuid1-2.38.1-5+b1            Negligible      None        CVE-2022-0563       https://security-tracker.debian.org/tracker/CVE-2022-0563           dpkg        debian:12       pkgdb
CVE-2022-0563           mount-2.38.1-5+b1               Negligible      None        CVE-2022-0563       https://security-tracker.debian.org/tracker/CVE-2022-0563           dpkg        debian:12       pkgdb
CVE-2022-0563           util-linux-2.38.1-5+b1          Negligible      None        CVE-2022-0563       https://security-tracker.debian.org/tracker/CVE-2022-0563           dpkg        debian:12       pkgdb
CVE-2022-0563           util-linux-extra-2.38.1-5+b1    Negligible      None        CVE-2022-0563       https://security-tracker.debian.org/tracker/CVE-2022-0563           dpkg        debian:12       pkgdb
CVE-2022-27943          gcc-12-base-12.2.0-14           Negligible      None        CVE-2022-27943      https://security-tracker.debian.org/tracker/CVE-2022-27943          dpkg        debian:12       pkgdb
```

Рис. 24. Некоторые из найденных уязвимостей

Тоесть anchore анализирует далеко не все контейнеры.

2.5. Docker Bench for Security

Так как Docker Bench Security необходимо запускать изнутри контейнера, а в выбранный образ не только не интерактивный (zig запускается один раз), но и отстуствует шелл впринципе (`busybox (x86_64)`) Пробовал:

- `/bin/bash`
- `/bin/sh`
- `sh`
- `/bin/ash`

Поэтому возмем образ от того же автора для той же цели, но на основе дебиана `kassany/bookworm-ziglang`

```
docker run --rm -it -v $(pwd):/app -w /app kassany/bookworm-
ziglang:latest bash
apt update
apt install git
```

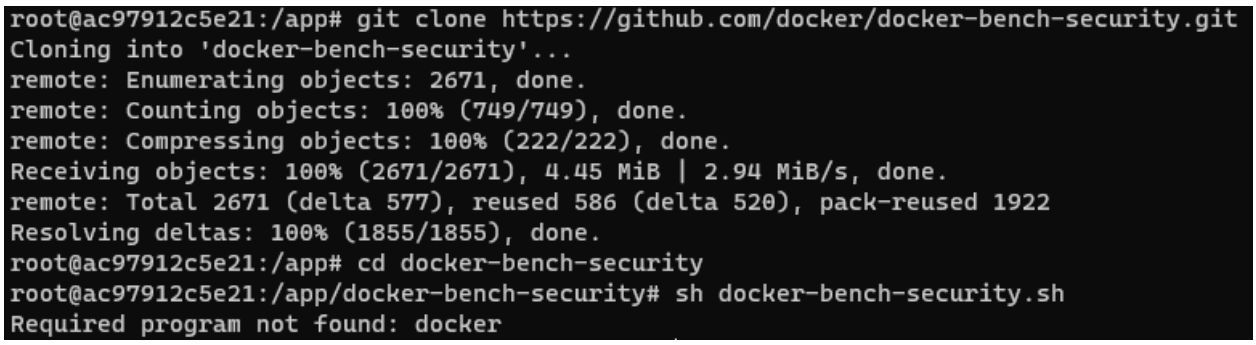


Рис. 25. Первый запуск

Ставим docker engine

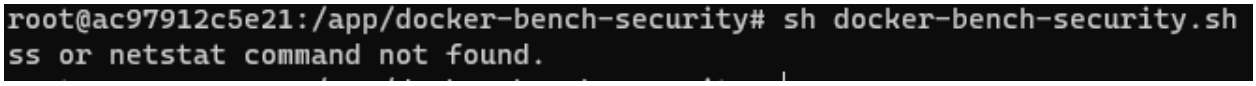


Рис. 26. Первый запуск

Отсюда я предполагаю что скрипт должен быть запущен на хостовой машине (либо используя контейнер docker-bench-security)

```
git clone https://github.com/docker/docker-bench-security.git
cd docker-bench-security
sudo sh docker-bench-security.sh
```

```
# ------------------------------------------------------------------------
# Docker Bench for Security v1.6.0
#
# Docker, Inc. (c) 2015-2023
#
# Checks for dozens of common best-practices around deploying Docker
containers in production.
# Based on the CIS Docker Benchmark 1.6.0.
# ------------------------------------------------------------------------

Initializing 2023-11-14T12:30:23+00:00


Section A - Check results
```

```
[INFO] 1 - Host Configuration
[INFO] 1.1 - Linux Hosts Specific Configuration
[WARN] 1.1.1 - Ensure a separate partition for containers has been
created (Automated)
[INFO] 1.1.2 - Ensure only trusted users are allowed to control Docker
daemon (Automated)
[INFO]       * Users: vagrant
[WARN] 1.1.3 - Ensure auditing is configured for the Docker daemon
(Automated)
[WARN] 1.1.4 - Ensure auditing is configured for Docker files and
directories -/run/containerd (Automated)
[WARN] 1.1.5 - Ensure auditing is configured for Docker files and
directories - /var/lib/docker (Automated)
[WARN] 1.1.6 - Ensure auditing is configured for Docker files and
directories - /etc/docker (Automated)
[WARN] 1.1.7 - Ensure auditing is configured for Docker files and
directories - docker.service (Automated)
[INFO] 1.1.8 - Ensure auditing is configured for Docker files and
directories - containerd.sock (Automated)
[INFO]       * File not found
[WARN] 1.1.9 - Ensure auditing is configured for Docker files and
directories - docker.socket (Automated)
[WARN] 1.1.10 - Ensure auditing is configured for Docker files and
directories - /etc/default/docker (Automated)
[INFO] 1.1.11 - Ensure auditing is configured for Dockerfiles and
directories - /etc/docker/daemon.json (Automated)
[INFO]       * File not found
[WARN] 1.1.12 - 1.1.12 Ensure auditing is configured for Dockerfiles
and directories - /etc/containerd/config.toml (Automated)
[INFO] 1.1.13 - Ensure auditing is configured for Docker files and
directories - /etc/sysconfig/docker (Automated)
[INFO]       * File not found
[WARN] 1.1.14 - Ensure auditing is configured for Docker files and
directories - /usr/bin/containerd (Automated)
[WARN] 1.1.15 - Ensure auditing is configured for Docker files and
directories - /usr/bin/containerd-shim (Automated)
```

```
[WARN] 1.1.16 - Ensure auditing is configured for Docker files and
directories - /usr/bin/containerd-shim-runc-v1 (Automated)
[WARN] 1.1.17 - Ensure auditing is configured for Docker files and
directories - /usr/bin/containerd-shim-runc-v2 (Automated)
[WARN] 1.1.18 - Ensure auditing is configured for Docker files and
directories - /usr/bin/runc (Automated)
[INFO] 1.2 - General Configuration
[NOTE] 1.2.1 - Ensure the container host has been Hardened (Manual)
[PASS] 1.2.2 - Ensure that the version of Docker is up to date (Manual)
[INFO]        * Using 24.0.7 which is current
[INFO]        * Check with your operating system vendor for support
and security maintenance for Docker

[INFO] 2 - Docker daemon configuration
[NOTE] 2.1 - Run the Docker daemon as a non-root user, if possible
(Manual)
docker-bench-security.sh: 37: [[: not found
[WARN] 2.2 - Ensure network traffic is restricted between containers
on the default bridge (Scored)
[PASS] 2.3 - Ensure the logging level is set to 'info' (Scored)
docker-bench-security.sh: 96: [[: not found
[PASS] 2.4 - Ensure Docker is allowed to make changes to iptables
(Scored)
docker-bench-security.sh: 118: [[: not found
[PASS] 2.5 - Ensure insecure registries are not used (Scored)
[PASS] 2.6 - Ensure aufs storage driver is not used (Scored)
[INFO] 2.7 - Ensure TLS authentication for Docker daemon is configured
(Scored)
[INFO]      * Docker daemon not listening on TCP
docker-bench-security.sh: 185: [[: not found
[INFO] 2.8 - Ensure the default ulimit is configured appropriately
(Manual)
[INFO]      * Default ulimit doesn't appear to be set
docker-bench-security.sh: 208: [[: not found
[WARN] 2.9 - Enable user namespace support (Scored)
[PASS] 2.10 - Ensure the default cgroup usage has been confirmed
```

```
(Scored)
[PASS] 2.11 - Ensure base device size is not changed until needed
(Scored)
docker-bench-security.sh: 276: [[: not found
[WARN] 2.12 - Ensure that authorization for Docker client commands
is enabled (Scored)
[WARN] 2.13 - Ensure centralized and remote logging is configured
(Scored)
[WARN] 2.14 - Ensure containers are restricted from acquiring new
privileges (Scored)
[WARN] 2.15 - Ensure live restore is enabled (Scored)
[WARN] 2.16 - Ensure Userland Proxy is Disabled (Scored)
[INFO] 2.17 - Ensure that a daemon-wide custom seccomp profile is
applied if appropriate (Manual)
[INFO] Ensure that experimental features are not implemented in
production (Scored) (Deprecated)

[INFO] 3 - Docker daemon configuration files
[PASS] 3.1 - Ensure that the docker.service file ownership is set to
root:root (Automated)
[PASS] 3.2 - Ensure that docker.service file permissions are
appropriately set (Automated)
[PASS] 3.3 - Ensure that docker.socket file ownership is set to
root:root (Automated)
[PASS] 3.4 - Ensure that docker.socket file permissions are set to
644 or more restrictive (Automated)
[PASS] 3.5 - Ensure that the /etc/docker directory ownership is set
to root:root (Automated)
[PASS] 3.6 - Ensure that /etc/docker directory permissions are set
to 755 or more restrictively (Automated)
[INFO] 3.7 - Ensure that registry certificate file ownership is set
to root:root (Automated)
[INFO]      * Directory not found
[INFO] 3.8 - Ensure that registry certificate file permissions are
set to 444 or more restrictively (Automated)
[INFO]      * Directory not found
```

```
[INFO] 3.9 - Ensure that TLS CA certificate file ownership is set to
root:root (Automated)
[INFO]      * No TLS CA certificate found
[INFO] 3.10 - Ensure that TLS CA certificate file permissions are set
to 444 or more restrictively (Automated)
[INFO]      * No TLS CA certificate found
[INFO] 3.11 - Ensure that Docker server certificate file ownership
is set to root:root (Automated)
[INFO]      * No TLS Server certificate found
[INFO] 3.12 - Ensure that the Docker server certificate file
permissions are set to 444 or more restrictively (Automated)
[INFO]      * No TLS Server certificate found
[INFO] 3.13 - Ensure that the Docker server certificate key file
ownership is set to root:root (Automated)
[INFO]      * No TLS Key found
[INFO] 3.14 - Ensure that the Docker server certificate key file
permissions are set to 400 (Automated)
[INFO]      * No TLS Key found
[PASS] 3.15 - Ensure that the Docker socket file ownership is set to
root:docker (Automated)
[PASS] 3.16 - Ensure that the Docker socket file permissions are set
to 660 or more restrictively (Automated)
[INFO] 3.17 - Ensure that the daemon.json file ownership is set to
root:root (Automated)
[INFO]      * File not found
[INFO] 3.18 - Ensure that daemon.json file permissions are set to 644
or more restrictive (Automated)
[INFO]      * File not found
[WARN] 3.19 - Ensure that the /etc/default/docker file ownership is
set to root:root (Automated)
[WARN]      * Wrong ownership for /etc/default/docker
[PASS] 3.20 - Ensure that the /etc/default/docker file permissions
are set to 644 or more restrictively (Automated)
[INFO] 3.21 - Ensure that the /etc/sysconfig/docker file permissions
are set to 644 or more restrictively (Automated)
[INFO]      * File not found
```

```
[INFO] 3.22 - Ensure that the /etc/sysconfig/docker file ownership is set to root:root (Automated)
[INFO]       * File not found
[PASS] 3.23 - Ensure that the Containerd socket file ownership is set to root:root (Automated)
[PASS] 3.24 - Ensure that the Containerd socket file permissions are set to 660 or more restrictively (Automated)

[INFO] 4 - Container Images and Build File
[INFO] 4.1 - Ensure that a user for the container has been created (Automated)
[INFO]      * No containers running
[NOTE] 4.2 - Ensure that containers use only trusted base images (Manual)
[NOTE] 4.3 - Ensure that unnecessary packages are not installed in the container (Manual)
[NOTE] 4.4 - Ensure images are scanned and rebuilt to include security patches (Manual)
[WARN] 4.5 - Ensure Content trust for Docker is Enabled (Automated)
[WARN] 4.6 - Ensure that HEALTHCHECK instructions have been added to container images (Automated)
[WARN]      * No Healthcheck found: [k0tran/ziglang:latest kassany/ziglang:latest]
[WARN]      * No Healthcheck found: [k0tran/ziglang:latest kassany/ziglang:latest]
[WARN]     * No Healthcheck found: [kassany/bookworm-ziglang:latest]
[WARN]      * No Healthcheck found: [aquasec/trivy:latest]
[WARN]      * No Healthcheck found: [postgres:9]
[INFO] 4.7 - Ensure update instructions are not used alone in the Dockerfile (Manual)
[INFO]           *  Update  instruction  found:  [kassany/bookworm-ziglang:latest]
[INFO]      * Update instruction found: [postgres:9]
[NOTE] 4.8 - Ensure setuid and setgid permissions are removed (Manual)
[PASS] 4.9 - Ensure that COPY is used instead of ADD in Dockerfiles (Manual)
```

```
[NOTE] 4.10 - Ensure secrets are not stored in Dockerfiles (Manual)
[NOTE] 4.11 - Ensure only verified packages are installed (Manual)
[NOTE] 4.12 - Ensure all signed artifacts are validated (Manual)

[INFO] 5 - Container Runtime
[INFO]   * No containers running, skipping Section 5

[INFO] 6 - Docker Security Operations
[INFO] 6.1 - Ensure that image sprawl is avoided (Manual)
[INFO]      * There are currently: 5 images
[INFO]      * Only 0 out of 5 are in use
[INFO] 6.2 - Ensure that container sprawl is avoided (Manual)
[INFO]      * There are currently a total of 0 containers, with 0 of
them currently running

[INFO] 7 - Docker Swarm Configuration
[PASS] 7.1 - Ensure swarm mode is not Enabled, if not needed
(Automated)
[PASS] 7.2 - Ensure that the minimum number of manager nodes have
been created in a swarm (Automated) (Swarm mode not enabled)
[PASS] 7.3 - Ensure that swarm services are bound to a specific host
interface (Automated) (Swarm mode not enabled)
[PASS] 7.4 - Ensure that all Docker swarm overlay networks are
encrypted (Automated)
[PASS] 7.5 - Ensure that Docker's secret management commands are used
for managing secrets in a swarm cluster (Manual) (Swarm mode not
enabled)
[PASS] 7.6 - Ensure that swarm manager is run in auto-lock mode
(Automated) (Swarm mode not enabled)
[PASS] 7.7 - Ensure that the swarm manager auto-lock key is rotated
periodically (Manual) (Swarm mode not enabled)
[PASS] 7.8 - Ensure that node certificates are rotated as appropriate
(Manual) (Swarm mode not enabled)
[PASS] 7.9 - Ensure that CA certificates are rotated as appropriate
(Manual) (Swarm mode not enabled)
[PASS] 7.10 - Ensure that management plane traffic is separated from
```

```
data plane traffic (Manual) (Swarm mode not enabled)



Section C - Score

[INFO] Checks: 86
[INFO] Score: -2
```

```
sudo sh docker-bench-security.sh -c container_images
```

```
# ------------------------------------------------------------------------
# Docker Bench for Security v1.6.0
#
# Docker, Inc. (c) 2015-2023
#
# Checks for dozens of common best-practices around deploying Docker
containers in production.
# Based on the CIS Docker Benchmark 1.6.0.
# ------------------------------------------------------------------------

Initializing 2023-11-14T12:32:33+00:00



Section A - Check results

[INFO] 4 - Container Images and Build File
[INFO] 4.1 - Ensure that a user for the container has been created
(Automated)
[INFO]      * No containers running
[NOTE] 4.2 - Ensure that containers use only trusted base images
(Manual)
[NOTE] 4.3 - Ensure that unnecessary packages are not installed in
the container (Manual)
[NOTE] 4.4 - Ensure images are scanned and rebuilt to include security
patches (Manual)
[WARN] 4.5 - Ensure Content trust for Docker is Enabled (Automated)
```

```
[WARN] 4.6 - Ensure that HEALTHCHECK instructions have been added to container images (Automated)
[WARN]      * No Healthcheck found: [k0tran/ziglang:latest kassany/ziglang:latest]
[WARN]      * No Healthcheck found: [k0tran/ziglang:latest kassany/ziglang:latest]
[WARN]     * No Healthcheck found: [kassany/bookworm-ziglang:latest]
[WARN]      * No Healthcheck found: [aquasec/trivy:latest]
[WARN]      * No Healthcheck found: [postgres:9]
[INFO] 4.7 - Ensure update instructions are not used alone in the Dockerfile (Manual)
[INFO]           *  Update  instruction  found:  [kassany/bookworm-ziglang:latest]
[INFO]      * Update instruction found: [postgres:9]
[NOTE] 4.8 - Ensure setuid and setgid permissions are removed (Manual)
[PASS] 4.9 - Ensure that COPY is used instead of ADD in Dockerfiles (Manual)
[NOTE] 4.10 - Ensure secrets are not stored in Dockerfiles (Manual)
[NOTE] 4.11 - Ensure only verified packages are installed (Manual)
[NOTE] 4.12 - Ensure all signed artifacts are validated (Manual)


Section C - Score

[INFO] Checks: 12
[INFO] Score: -2
```

3. Подведение итогов

	Docker Scout	**Snyk**	**Trivy**	**Anchore**	**Docker Bench**
FOSS	-	+-	+	+-	+
Kubernetes	-	+	+	+**	+***
CI/CD	+	+	+	+	+

Оф. репозитории Docker	+	+	+	+	?
CVE и CWE	+	+	+*	+	-
Производительность	+	+	+	−1000	+
Простота	+-	+	+	−10	+
Вид	Web+CLI	CLI	CLI	Cont+CLI	Script/ Cont
Мультиплатформенность	+	+	+	+	-
VPN	+	+	+	+	+
Обновления бд	+	+	+	-	+
Доп. функционал	платно	платно	бесплатно	платно	бесплатно

* - есть, но не в моем случае ** - обещания есть, платно. *** - kube-bench